U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

OFFICE OF NUCLEAR REACTOR REGULATION

NEW

Section 7.8. Diverse Instrumentation and Control Systems

Review Responsibilities

Primary — Instrumentation and Controls Branch (HICB)

Secondary — None

I. Areas of Review

This SRP section describes the review process and acceptance criteria for the diverse instrumentation and control (I&C) systems and equipment provided for the express purpose of protecting against potential common-mode failures of protection systems. The following systems are covered by this section:

1. Anticipated transient without scram (ATWS) mitigation systems required for compliance with 10 CFR 50.62. As defined in 10 CFR 50.62, an ATWS event is an anticipated operational occurrence followed by failure of the reactor trip portion of the protection system. 10 CFR 50.62 identifies design requirements for ATWS mitigation systems and equipment.

2. Diverse manual controls and displays provided to comply with the NRC position on defense-in-depth and diversity (D-in-D&D) as described in the Staff Requirements Memorandum (SRM) regarding SECY-93-087. These systems are to be independent and diverse from the safety computer system, and are to be located in the main control room for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions.

3. Diverse actuation systems (DAS) are those automatic systems provided solely for the purpose of meeting the NRC position on D-in-D&D. DAS and ATWS mitigation system functions may be combined into a single system. The reactor trip system (RTS), engineered safety features actuation system (ESFAS), control system, or other diverse I&C systems may perform DAS functions to meet the NRC position on D-in-D&D. Diverse I&C system functions performed by these other systems are not within the scope of this section. The diverse I&C functions of these systems should meet the criteria applicable to the systems as a whole. The requirements for these systems and the Staff's review are found in the SRP sections for the individual systems.

The objectives of this review are to ensure that the ATWS mitigation systems and equipment are designed and installed in accordance with the requirements of 10 CFR 50.62, and that other diverse I&C systems within the scope of this section comply with the guidance of the NRC position on D-in-D&D.

SRP Section 7.0 describes the coordination of reviews, including the information to be reviewed and the scope required for each of the different types of applications that the Office of Nuclear Reactor Regulation (NRR) may review. Refer to that section for information regarding how the areas of review are affected by the type of application under consideration and for a description of coordination between HICB and other branches.

In addition to the coordination described in SRP Section 7.0, the Reactor Systems Branch (SRXB) evaluates the following aspects of the diverse I&C systems:

1. The ATWS mitigation protective functions are reviewed to confirm that they meet the requirements of 10 CFR 50.62. The thermal/hydraulic analytical basis for ATWS is reviewed to verify that the ATWS analysis is consistent with the analyses presented or referenced in the safety analysis report (SAR) Chapter 15 for anticipated operational occurrences, and to verify the adequacy of the design of mechanical systems used to mitigate ATWS.

2. The adequacy of the set of manual control and display functions is reviewed to confirm it is sufficient to monitor the plant states and to actuate systems required by the control room operators to place the nuclear plant in a hot-shutdown condition and to control the following critical safety functions: reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity.

3. For plants with a digital computer-based RTS or ESFAS, DAS functions are reviewed to confirm that they are consistent with the portions of the accident analysis that support the D-in-D&D analysis.

II. Acceptance Criteria

Acceptance criteria and guidelines applicable to diverse I&C systems are identified in SRP Section 7.1. The review of Section 7.1 of the SAR confirms that the appropriate acceptance criteria and guidelines have been identified for these systems. The review of the diverse I&C systems confirms that these systems conform to the requirements of the acceptance criteria and guidelines.

Acceptance criteria for the review of diverse I&C systems are the relevant requirements of the following regulations:

1. Acceptance criteria applicable to all diverse I&C system functions

10 CFR 50.55a(a)(1), "Quality Standards."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Station." For diverse I&C systems, the only applicable requirement from ANSI/IEEE 279 is item 4.7.2, "Isolation Devices."

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 13, "Instrumentation and Control."

General Design Criterion 19, "Control Room."

General Design Criterion 24, "Separation of Protection and Control Systems."

Note that the design of the diverse I&C systems must be such that the protection system continues to meet the requirements of 10 CFR 50 Appendix A, "General Design Criteria for Nuclear Power Plants," Section III, "Protection and Reactivity Control Systems." Review of the reactor protection system for these areas of conformance is addressed in SRP Sections 7.2 and 7.3.

2. Acceptance criteria applicable to all diverse I&C systems proposed for design certification under 10 CFR 52, in addition to those listed in 1 above

10 CFR 52.47(a)(1)(iv), "Resolution of Unresolved and Generic Safety Issues."

10 CFR 52.47(a)(1)(vi), "ITAAC in Design Certification Applications."

10 CFR 52.47(a)(1)(vii), "Interface Requirements."

10 CFR 52.47(a)(2), "Level of Detail."

3. Acceptance criteria applicable to all diverse I&C systems proposed as part of combined license applications under 10 CFR 52.79(c), in addition to those listed in 1 above

10 CFR 52.79(c), "ITAAC in Combined Operating License Applications."

4. Acceptance criteria applicable to ATWS mitigation functions, in addition to the applicable criteria listed in 1 above

10 CFR 50.62, "Requirements for reduction of risk from ATWS events for light-water-cooled nuclear power plants."

5. Acceptance criteria applicable to manual control and display functions, in addition to those listed in 1 above

Item II.Q, "Defense Against Common-Mode Failures in Digital Instrument and Control Systems," of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." SRM requirements applicable to diverse I&C system manual control and display functions are as follows:

"A set of displays and controls located in the main control room shall be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions.

"The displays and controls shall be independent and diverse from the safety computer systems."

6. Acceptance criteria applicable to DAS functions, in addition to those listed in 1 above

Item II.Q, "Defense Against Common-Mode Failures in Digital Instrument and Control Systems," of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." SRM requirements applicable to DAS functions are as follows:

"If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure [as the safety system][1] shall be required to perform either the same function [as the safety system function that is vulnerable to common mode failure] or a different function.

"The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary functions under the associated event conditions."

III. Review Procedures

Section 7.1 describes the general procedures to be followed in reviewing any I&C system. Procedures for reviewing each acceptance criterion of 10 CFR 50 and 10 CFR 52 are provided in Appendix 7.1-A. Therefore, review procedures specific to any given diverse I&C system can be synthesized from Appendix 7.1-A. Note that while compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," is required only for protection systems, the criteria of ANSI/IEEE Std 279 and Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems" (which endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations") address considerations that may be used as guidance, where appropriate, for reviewing any diverse I&C application.

This part of Section 7.8 provides a review procedure for conformance of diverse I&C systems with the requirements of 10 CFR 50.62 and the SRM regarding SECY-93-087. This part of Section 7.8 highlights specific topics that should be emphasized in the application of the Appendix 7.1-A review procedures to diverse I&C systems.

Major design considerations that should be emphasized in the review of any diverse I&C system are identified below.

- Design basis — Design bases should be described in the SAR for each diverse I&C system. The design basis should, as a minimum, address the following topics:
  - The specific design requirements identified in 10 CFR 50.62.

[1]Bracketed phrases added for clarity.

– Identification of conditions which require protective action by the diverse I&C systems. For DAS these events are identified in the applicant/licensee's D-in-D&D analysis. For ATWS mitigation systems these events are limited to anticipated operational occurrences, defined in the Definitions and Explanations section of 10 CFR 50 Appendix A as those conditions of normal operation which are expected to occur one or more times during the life of the nuclear power unit, and include but are not limited to loss of power to all recirculation pumps, tripping of the turbine generator, isolation of the main condenser, and loss of all offsite power.

– Identification by the applicant/licensee of the bounding events and their bases in the analyses that are presented or referenced in SAR Chapter 15. The reviewer should confirm with SRXB that the analytical basis for each diverse I&C system is acceptable and consistent with the Chapter 15 analysis, and should confirm with SRXB and Plant Systems Branch (SPLB) that the design of the mechanical systems used for ATWS mitigation is acceptable.

– Identification of the range of transient and steady-state conditions for both the energy supply and the environment during normal, abnormal, and accident conditions under which the system must perform. The environmental qualification basis for the ATWS mitigating equipment should be derived from the analysis of the effects of the anticipated operational occurrences.

– Identification of the performance requirements. The submittal should identify performance requirements for which credit is taken in the mitigation of design basis events (e.g., dynamic response and accuracy). The review should confirm that the applicant/licensee verifies conformance to these requirements by validation testing and surveillance.

- Quality of components and modules — Generic Letter 85-06 provides acceptable guidance for the quality assurance of diverse I&C systems and components.

- System testing and surveillance — The applicant/licensee should have identified the test, maintenance, surveillance, and calibration procedures. These provisions should be consistent with the guidance of Generic Letter 85-06. The ATWS mitigation system should be testable at power (up to, but not necessarily including, the final actuation device).

- Defense-in-depth and diversity analysis — The diverse I&C system designs should be consistent with the assumptions of the applicant/licensee's D-in-D&D analysis, if one has been performed. For example, diverse I&C system equipment should be environmentally qualified for the environments in which the D-in-D&D analysis assumes they will operate.

- Use of digital systems — See Appendix 7.0-A.

- Power supply availability — The reviewer should confirm with EELB that power sources will be available during and following a loss of offsite power.

- Environmental qualification — The diverse I&C system equipment as installed should be qualified for the environment that could exist during the events for which the equipment is assumed to respond.

- System status — Information should be available in the control room to indicate the operation of the diverse I&C systems. This review may involve the considerations included in emergency operating procedures.

- Potential for inadvertent actuation — The diverse I&C systems design should limit the potential for inadvertent actuation and challenges to safety systems. Diverse I&C systems should be designed to initiate after the primary protection system actuation conditions are exceeded. (The use of a primary protection signal sensor to simultaneously initiate diverse I&C functions is acceptable.)

Additional major design considerations that should be emphasized in the review of ATWS mitigation systems are identified below.

- Independence from the RTS — The ATWS mitigation equipment should be independent and diverse from the RTS from the sensor output to the final actuation device. See Appendix 7.1-B item 8 or Appendix 7.1-C item 24.

- Manual initiation capability — The ATWS mitigation systems should include the capability for initiation from the control room.

- Completion of protective action — The ATWS mitigation logic should be designed such that once ATWS mitigation is initiated the mitigation will go to completion.

  If the applicant/licensee has provided a D-in-D&D analysis, the diversity provided in the ATWS mitigation system design should be consistent with the assumptions of that analysis.

  Where a D-in-D&D analysis is not provided the following diversity criteria should be met:

  – Equipment diversity should be provided to the extent reasonable and practicable to minimize the potential for common-mode failures.

  – Equipment diversity is required from the sensors/transmitters to and including the components used to interrupt control rod power or vent the scram air header.

  – For interruption of control rod power, obtaining circuit breakers from different manufacturers is not, in and of itself, sufficient to provide the required diversity.

  – For mitigating systems other than diverse reactor trip systems (e.g., auxiliary feedwater) diversity is required from the sensors to, but not including, the final actuation device.

  – Sensors need not be of a diverse design or manufacturer.

  – Existing RTS sensing lines may be used for ATWS mitigation instruments.

  – Sensors/transmitters and sensing lines should be selected such that adverse interactions with existing control systems are avoided.

  – Logic and actuation device power for the ATWS mitigation system must be from an instrument power supply independent from the power supplies for the existing RTS; existing RTS sensor and instrument channel power supplies may be used provided the possibility of common-mode failure is prevented.

If the ATWS system is explicitly addressed as part of a D-in-D&D analysis, then that analysis provides the basis for the assessing the adequacy of diversity between the ATWS mitigation system and the RTS.

Therefore, separate evaluation of the ATWS mitigation system against the above eight diversity criteria is unnecessary if the D-in-D&D analysis is provided.

Additional major design considerations that should be emphasized in the review of manual controls and displays are identified below.

- The manual controls and displays should meet the criteria outlined in BTP HICB-19.

In each safety review, the Staff should determine the elements of the design that require additional review emphasis. Typical reasons for such a non-uniform emphasis are the introduction of new design features or the utilization in the design of features previously reviewed and found acceptable. However, in all cases, the review must be sufficient to conclude conformance to the acceptance criteria, i.e., the requirements of the Code of Federal Regulations.

IV. Evaluation Findings

The Staff verifies that sufficient information has been provided and the review supports the following conclusions as stated in the SER:

Evaluation findings applicable to any diverse I&C system:

> The NRC staff conducted a review of these systems for conformance to the guidelines in the regulatory guides and industry codes and standards applicable to these systems. The Staff concluded that the applicant/licensee adequately identified the guidelines applicable to these systems. Based upon the review of the system design for conformance to the guidelines, the Staff finds that there is reasonable assurance that the systems fully conform to the guidelines applicable to these systems. Therefore, the Staff finds that these requirements of General Design Criteria (GDC) 1 and 10 CFR 50.55a(a)1 have been met.
>
> The diverse I&C systems are appropriately isolated from safety systems. Therefore, the Staff concludes that the isolation of these systems from safety systems satisfies the requirements of 10 CFR 50.55a(h) and the requirements of GDC 24.
>
> Based on the applicant/licensee's commitment to the quality assurance guidance of Generic Letter 85-06, the Staff finds that the quality assurance requirements of GDC 1 have been met.
>
> Based on the review of diverse I&C system status information, manual initiation capabilities, and provisions to support safe shutdown, the Staff concludes that information is provided to monitor the system over the anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety. Appropriate controls are provided for manual initiation of diverse I&C functions. The diverse I&C systems appropriately support actions to operate the nuclear power unit safety under normal conditions and to maintain it in a safe condition under accident conditions. Therefore, the Staff finds that the design of the diverse I&C systems satisfies the requirements of GDC 13 and 19.
>
> Based on the licensee's commitment to periodically test the diverse I&C systems from end-to-end [summarize the specific commitment], the Staff concludes that an acceptable level of availability for the system can be maintained.

Note: the following finding applies only to systems involving digital computer-based components.

> Based on the review of software development plans and the inspections of the computer development process and design outputs, the Staff concludes that the computer systems meet the

guidance of Reg. Guide 1.152. Therefore, the special characteristics of computer systems have been adequately addressed, and the Staff finds that the diverse I&C systems satisfy these requirements of GDC 1.

Additional evaluation findings applicable to all diverse I&C systems proposed in design certification applications under 10 CFR 52:

The diverse I&C systems design appropriately addresses the applicable unresolved and generic safety issues. Therefore, the Staff finds that the diverse I&C systems satisfy the requirements of 10 CFR 52.47(a)(1)(iv).

The review of the diverse I&C systems examined the proposed inspections, tests, analyses, and acceptance criteria (ITAAC). Based upon the review and coordination with those having primary responsibility for ITAAC, the Staff concludes that if the inspections, tests, and analyses are performed and the acceptance criteria met, the plant will operate in accordance with the [design certification OR combined license]. Therefore, the Staff finds that the diverse I&C systems satisfy the requirements of [10 CFR 52.47(a)(1)(vi) OR 10 CFR 52.79(c)].

The application for design certification does not seek certification for the following portions of the diverse I&C systems [insert list]. Based upon review of the completed safety analysis, the Staff finds that the requirements for these portions of the design were sufficiently detailed. Therefore, the Staff finds that the design of the diverse I&C systems satisfies the requirements of 10 CFR 52.47(a)(1)(vii).

Based upon an initial review of the scope and content of the material submitted by the applicant, and completed review with respect to the technical items above, the Staff finds that the application contained appropriate detail about the diverse I&C systems design to satisfy the requirements of 10 CFR 52.47(a)(2).

Additional evaluation findings applicable to ATWS mitigation systems:

The ATWS mitigation system instrumentation includes [summarize the basic functions and elements of the I&C system design submitted for review]. Based on the review of these functions and the design bases submitted by the applicant, the Staff concluded that the ATWS mitigation design includes an appropriate set of functions.

Based on review of the interfaces of the ATWS mitigation system and equipment with the RTS, the Staff concludes that the separation and independence of the RTS is not compromised by the ATWS mitigation system design. Where isolation devices are provided in the RTS to support ATWS mitigation interfaces, the isolation devices are applied and qualified to the guidelines of BTP HICB-11.

Based upon the above items, the Staff concludes that the design of the ATWS mitigation system is acceptable and satisfies the specific design requirements identified in 10 CFR 50.62 for [identify reactor type].

Additional evaluation findings applicable to diverse I&C system manual controls and displays:

Based on review of the design bases submitted by the applicant, the Staff concludes that the manual controls and displays are acceptable, independent and diverse from the safety computer system, and sufficient for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. Therefore, the Staff concludes that the manual controls and displays fulfill the requirements of the Staff Requirements Memorandum on SECY 93-087, item II.Q.

Additional evaluation findings applicable to DAS:

> Based on review of the design bases submitted by the applicant, the Staff concludes that the DAS is acceptable. The functional requirements, independence requirements, and diversity requirements for this system are consistent with the applicant's defense-in-depth and diversity analysis, and fulfill the applicable requirements of the SRM on SECY-93-087, item II.Q.

Note: the following conclusion is applicable to all applications.

> The conclusions noted above for the diverse I&C systems are applicable to all portions of the systems except for the following, for which acceptance is based upon prior NRC review and approval as noted [List applicable system or topics and identify references].

V. Implementation

Except in those cases in which the applicant/licensee proposes an acceptable alternative method for complying with specified portions of the NRC's regulations, the method described herein will be used by the NRC staff in its evaluation of conformance with NRC regulations.

Implementation schedules for conformance to the method discussed herein are contained in 10 CFR 50.62, the 10 CFR 50.62 considerations identified in the Federal Register Notice (FR Vol. 49, No. 124), and Generic Letter 85-06.

VI. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

Federal Register 49 FR 26042. "Statement of Considerations for the ATWS Rule," 10 CFR 50.62.

Generic Letter 85-06. "Quality Assurance Guidance for ATWS Equipment that is not Safety-Related," April 16, 1986.

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.75. "Physical Independence of Electrical Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1978.

SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." April 2, 1993.

Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." July 15, 1993.